**REMARKS**

In the June 16, 2004 Office Action, the Examiner noted that claims 1-29 were pending in the application; objected to claim 1 due to a spelling error; rejected claims 1-4, 9, 15-17 and 24-29 under 35 USC § 102(e); and rejected claims 5-8, 10-14 and 18-23 under 35 USC § 103(a). In rejecting the claims, U.S. Patents 6,292,092 to <u>Chow et al.</u> and 5,742,685 to <u>Berson et al.</u> (References A and B, respectively) were cited. Claims 5, 10 and 11 have been cancelled and claims 30-33 have been added. Thus, claims 1-4, 6-9 and 12-33 remain in the case. The Examiner's rejections are traversed below.

**The Application**

The subject application is directed to authenticating a user based on encoded information possessed by the user and information maintained by a certification institution. As illustrated in Fig. 1, identification information entered by a user is processed by an output unit which produces signature information that includes program information for certification of the signature. In the preferred embodiment, the output unit produces a two-dimensional bar code. In addition, the output unit, e.g., a user's PC 11 in Fig. 2, communicates with a certification unit which maintains database 16 and issues certification information to be included in the two-dimensional bar code. The two-dimensional bar code output by the user's PC can be used in conjunction with the signature reception device 102, POS terminal 103 or ATM 104, all of which include a bar code reader.

A system according to the invention is illustrated in Fig. 13. As described on pages 32-47 with reference to the flowcharts in Figs. 17-24 and the explanatory diagrams in Figs. 14-16, the user's personal computer system which includes an image scanner, printer and bar code reader generates the two-dimensional bar code and is connected via network 107 with at least digital registered seal management device 106. The same network or one or more other networks may connect the signature reception device 102, POS terminal 103, ATM 104 and a financial process device 105. As described in the paragraph spanning pages 23 and 24, the program which generates the blind information is executed on the user PC 101. The certification institution stores a hash function, encryption key and blind information (authentication information) generated using the hash function and the encryption key, all of which are received from the user's PC. The certification institution issues additional information that is incorporated into the two-dimensional bar code to certify that the user is registered with the certification institution.

Subsequently, one of the devices 102, 103, 104 or 105 reads the two-dimensional bar code to obtain the encrypted data and information used to generate a program to hash and encrypt use information, such as the present date and time or a random number to generate encrypted use information. This is sent together with the original use information, the encrypted authentication information and the certification information as signature information to the certification institution which verifies the correctness of the signature information, and then the program used by the input device is erased. The certification institution verifies correctness of the signature information by decrypting the encrypted authentication information using an encryption (or decryption) key to reproduce the original authentication information which is then re-encrypted using the hash function and encryption key supplied by the user for comparison with the encrypted authentication information that was originally supplied by the user and stored in database 120. The certification institution also uses the hash function and encryption key to process the use information for comparison with the use information sent by device 102, 103, 104 and 105. When all of the information received by the certification institution matches the encrypted (blind) information stored by the certification institution and the encrypted (blind) authorization and use information regenerated by the certification institution, the transaction is approved.

**The Prior Art**

### U.S. Patent 6,292,092 to Chow et al.

The Chow et al. patent is directed to a secure personal identification instrument which includes a photograph for personal signature and personal information, such as name, birth date and place, blood type and ID number. In addition, authentication information is stored in, e.g., a two-dimensional bar code, an integrated circuit, a magnetic stripe, or an OCR code which preferably is encrypted. The identification instrument is presented at an authentication station which decodes the stored information and compares it with, e.g., a digitized scan of the photograph of the user which itself can be compared with the appearance of the user. The user may supply a pass code that is required for properly decoding the encrypted information.

### U.S. Patent 5,742,685 to Berson et al.

The Berson et al. patent is directed to verifying an identification card which uses date and time information to prevent illegal use.

**Rejections under 35 USC § 102**

In items 4-12 on pages 2-4 of the Office Action, claims 1-4, 9, 15-17 and 24-29 were rejected under 35 USC § 102(e) as anticipated by <u>Chow et al.</u> Nothing was cited or has been found in <u>Chow et al.</u> teaching or suggesting that the signature information includes "program information for generation of illegal use prevention information" (e.g., claim 1, lines 5-6) as described at, e.g., page 34, line 11 to page 36, line 9 and page 38, lines 13-19). Since claims 9, 24, 25, 27 and 28 recite limitations that also require program information, it is submitted that claims 1, 9, 24, 25, 27 and 28, as well as claims 2-4 which depend from claim 1 patentably distinguish over <u>Chow et al.</u>

Claim 15 recites "a management unit managing the blind information of the authentication information" (claim 15, last two lines). As discussed above, <u>Chow et al.</u> does not describe any verification of the information stored in the identification instrument by referencing another database, but only by verifying that the encrypted information matches the signature or photograph in a self-contained apparatus. This simplifies the process of authentication, but is not as secure as the invention.

Claims 26 and 29 similarly recite managing information and add comparing the information that is stored separately. Therefore, it is submitted that claims 15, 26 and 29, in addition to claims 16 and 17 which depend from claim 15 patentably distinguish over <u>Chow et al.</u>

**Rejections under 35 USC § 103**

In paragraphs 13-16 on pages 5 and 6 of the Office Action, claims 5-8 and 10-14 were rejected under 35 USC § 103(a) as unpatentable over <u>Chow et al.</u> in view of <u>Berson et al.</u> Claims 5, 10 and 11 have been cancelled and therefore, only claims 6-8 and 12-14 will be addressed.

It is submitted that nothing in <u>Berson et al.</u> overcomes the deficiencies of <u>Chow et al.</u> discussed above. Since claims 6-8 depend from claim 1, claims 12 and 13 depend from claim 9 and claim 14 depends from claim 15, it is submitted that claims 6-8 and 12-14 patentably distinguish over the prior art at least for the reasons discussed above.

In paragraphs 17 and 18 on page 6 of the Office Action, claims 18-23 were rejected under 35 USC § 103(a) as unpatentable over <u>Chow et al.</u> Since claims 18-23 depend from claim 15, it is submitted that claims 18-23 patentably distinguish over <u>Chow et al.</u> for at least the reasons discussed above with respect to claim 15.

**New Claims**

Claims 30-33 have been added as claims dependent from claims 1 and 9. Therefore, claims 30-33 patentably distinguish over the prior art at least for the reasons discussed above with respect to claims 1 and 9.

**Summary**

It is submitted that the references cited by the Examiner, taken individually or in combination, do not teach or suggest the features of the present claimed invention. Thus, it is submitted that claims 1-4, 6-9 and 12-33 are in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 9/16/04

By: Richard A. Gollhofer.
Registration No. 31,106

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Trademarks, 2900 Crystal Drive, Arlington, VA 22202-3514
on SEPTEMBER 16 , 2004
STAAS & HALSEY LLP
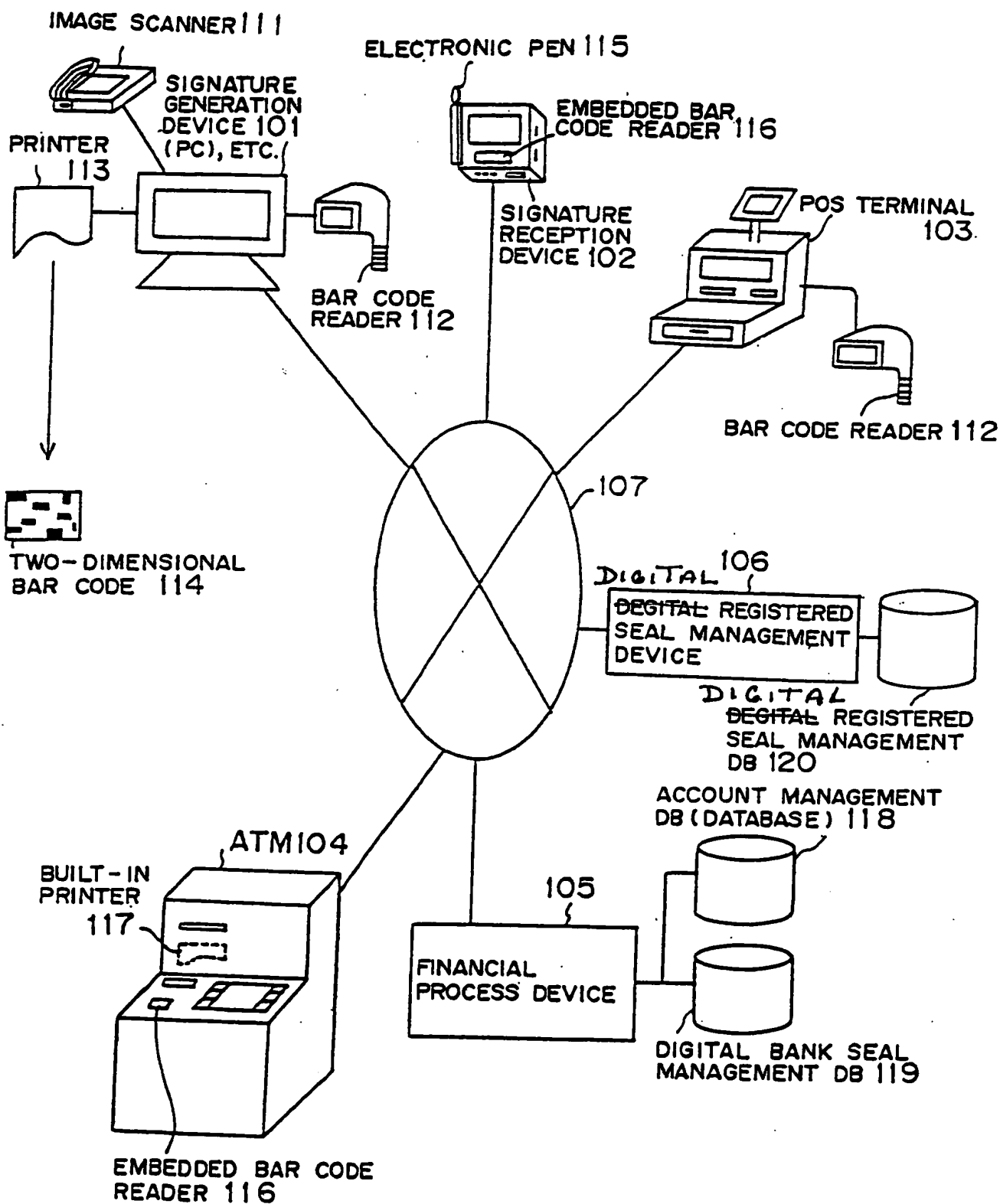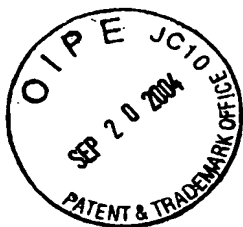By: Michelle Bryant
Date SEptEmber 16, 2004

12

FIG. 13